Amendment to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (currently amended) A method for ordering, authorizing, and delivering goods and services using a mobile station, comprising:

accessing a gateway by the mobile station and transmitting an identification code for mobile station to the gateway;

verifying the identity of the mobile station by the gateway by accessing an authentication center of a cellular network and comparing mobile station generated variables computed by the mobile station with gateway generated variables computed by the gateway;

verifying the legitimacy of the gateway by the mobile station by comparing the variables computed by the gateway with the variables computed by the mobile station;

requesting a digital certificate by the mobile station from the gateway used to order and authorize a product or service from a service provider;

delivering a digital certificate to the mobile station by the gateway when the identity of the mobile station have been verified; ~~and~~

requesting a product or service from the service provider; and

transmitting a digital signature by the mobile station accompanied by the digital certificate for a signature verification key as authorization to said service provider.

2. (previously presented) The method recited in claim 1, wherein the verifying the legitimacy of the gateway by the mobile station by comparing the variables computed by the gateway with the variables computed by the mobile station, further comprises:

transmitting from the mobile station to the gateway a session identification and a mobile subscriber identifier;

transmitting the mobile subscriber identifier from the gateway to the authentication center;

transmitting from the authentication center to the gateway a random number (RAND), a signed response (SRES), and an encryption key;

computing a variable MI by the gateway and transmitting the variable MI and the random number to the mobile station;

computing a variable MI' by the mobile station; and

verifying the legitimacy of the gateway when the variable MI equals the variable MI'.

3. (currently amended) The method recited in claim 2, wherein ~~the integrity~~ an integrity key (K) is computed by both the mobile station and the authentication

center as a function of RAND and Ki, where RAND is a random number issued by the authentication center, and Ki is a secret key contained within the authentication center and the mobile station.

4. (previously presented) The method recited in claim 3, where an integrity key (K) is transmitted by the authentication center to the gateway.

5. (original) The method recited in claim 1, further comprising:

computing a digital certificate by the gateway certifying the mobile station's public key(PK);

computing a variable M3 by the gateway and transmitting the variable M3 and the digital certificate to the mobile station;

computing a variable M3' by the mobile station;

verifying the legitimacy of the gateway when the variable M3 equals the variable M3'.

6. (original) The method recited in claim 5, wherein the variables M3 and M3' are computed using the formula M3 = M3' = MAC (K, C), where MAC is a message authentication code function, K is an integrity key and C is the digital certificate created by the gateway to certify PK.

7. (previously presented) The method recited in claim 1, wherein verifying the identity of the mobile station by the gateway accessing an authentication center and comparing variables computed by the mobile station and variables computed by the gateway, further comprises:

transmitting in at least one message a signed response, a public key and a variable M2 computed by the mobile station to the gateway;

computing a variable M2' by the gateway;

comparing the variable M2 and the variable M2'; and

verifying the identity of the mobile station when variable M2 is equal to variable M2'.

8. (original) The method recited in claim 7, wherein variables M2 and M2' are computed using the formula M2 = M2' = MAC (K, {SRES}, PK, [{restrictions}], [alias]), wherein MAC is a message authentication code function, SRES is a signed response, K is an integrity key, PK is a public key, restrictions are limits on the certificate and alias is an alternate identification for the mobile station.

9. (previously presented) The method recited in claim 1, wherein transmitting the digital signature, accompanied by the digital certificate for the signature verification key to said service provider, further comprises:

transmitting the certificate with a request for a product or service;

receiving an invoice from the service provider indicating a price for the product or service;

computing a digital signature on the invoice;

approving the invoice by transmitting the digital signature to the service provider; and

accepting delivery of the product or service by a buyer.

10. (previously presented) The method recited in claim 9, wherein the service provider upon transmission of the digital signature, further comprises:

verifying the digital signature;

verifying that restrictions associated with the digital certificate are not violated; and

creating an accounting record for the product or service sold.

11. (previously presented) The method recited in claim 10, further comprising:

transmitting from the service provider to the gateway the accounting record having an invoice and digital signature of a customer of a home network operator service;

determining by the gateway that a corresponding record exists in a local database and the validity of the digital signature;

determining whether the invoice violates any restrictions contained in the corresponding record;

crediting the service provider with an amount equal to that in the invoice; and

billing the buyer with the amount of the invoice.

12. -13. (canceled)

14. (previously presented) A system for ordering, authorizing and delivering goods and services using a mobile station, comprising:

a cellular network authentication module to verify that the mobile station is permitted to access a telecom infrastructure;

a mobile station certificate acquisition module to request a digital certificate for the mobile station from a gateway; and

a gateway certificate generation module to verify that the mobile station is authorized to receive the digital certificate by transmitting a mobile subscriber identifier received from the mobile station to an authentication center, calculate variables based on information received from the authentication center and compare them to variables computed by the mobile station, and issue the digital certificate to the mobile station when the variables match,

wherein the mobile station verifies the legitimacy of the gateway by comparing the variables calculated by the gateway with the variables computed by the mobile station, the mobile station requesting a product or service from a service provider and transmitting a digital signature accompanied by the digital certificate for a signature verification key as authorization to the service provider.

15. (original) The system recited in claim 14, wherein the mobile station certificate acquisition module verifies that the gateway is authorized to issue the digital certificate through the use of comparing variables computed by the gateway and the mobile station.

16. (previously presented) The system recited in claim 15, further comprising:

a purchase module to request the purchase of a good or service from a service provider, present the digital certificate to the service provider, receive an invoice and provide the service provider with a digital signature approving the purchase of the good or service;

a sales module to verify the validity of the digital certificate and the validity of the digital signature, issue an invoice, generate an accounting record and deliver a product or service;

a billing module to transmit to the gateway the accounting record and

receive a response indicating if the accounting record has been approved for payment; and

a gateway billing module to verify the accounting record and an accompanying signature, and issue a credit to the service provider and debit to a buyer when the accounting record and the accompanying signature are verified.

17. (previously presented) The system recited in claim 16, wherein the gateway certificate generation module transmits a mobile subscriber identifier to the authentication center, receives a random number, a signed response and an encryption key from the authentication center, computes a variable MI, M2', and M3 and verifies the validity of the mobile station by comparing variable M2 received from the mobile station with variable M2'.

18. (original) The system recited in claim 14, wherein the mobile station further comprises:

a subscriber identification module (SIM) used to compute a signed response and a ciphering key based on a secret key, installed by a home network operator service in the subscriber identification module upon signing up for a service plan, and a random number obtained from an authentication center in the home network operator service;

an A3 algorithm module, contained in the SIM, is used to compute the signed response; and

an A8 algorithm module, contained in the SIM, is used to compute the ciphering key, wherein through the transmission of signed responses to and from the mobile station a telecommunication infrastructure is able to verify that the mobile station is authorized to access the telecommunication infrastructure and the gateway.

19. (previously presented) A computer program embodied on a computer readable medium and executable by a computer for ordering, authorizing and delivering goods and services using a mobile station, comprising:

a cellular network authentication code segment to verify that the mobile station is permitted to access a telecom infrastructure;

a mobile station certificate acquisition code segment to request a digital certificate for the mobile station from a gateway; and

a gateway certificate generation code segment to verify that the mobile station is authorized to receive the digital certificate by transmitting a mobile subscriber identifier received from the mobile station to an authentication center, calculate variables based on information received from the authentication center and compare them to variables computed by the mobile station, and issue the digital certificate to the mobile station when the variables match.

wherein the mobile station verifies the legitimacy of the gateway by comparing the variables calculated by the gateway with the variables computed by the mobile station, the mobile station requesting a product or service from a service provider and transmitting a digital signature accompanied by the digital certificate for a signature verification key as authorization to the service provider.

20. (original) The system recited in claim 19, wherein the mobile station certificate acquisition code segment verifies that the gateway is authorized to issue

the digital certificate through the use of comparing variables computed by the gateway and the mobile station.

21. (previously presented) The computer program recited in claim 19, further comprising:

a purchase code segment to request the purchase of a good or service from a service provider, present the digital certificate to the service provider, receive an invoice and provide the service provider with a digital signature approval the purchase of the good or service;

a sales code segment to verify the validity of the digital certificate and the validity of the digital signature, issue an invoice, generate an accounting record and deliver a product or service;

a billing code segment to transmit to the gateway the accounting record and receive a response indicating if the accounting record has been approved for payment; and

a gateway billing code segment to verify the accounting record and an accompanying signature, and issue a credit to the service provider and debit to a buyer when the accounting record and the accompanying signature are verified.

22. (previously presented) The computer program recited in claim 20, wherein the mobile station certificate acquisition code segment transmits a session identification and a mobile subscriber identifier to the gateway, receives a random

number and a variable MI from the gateway and verifies that the gateway is authentic by computing and comparing the variable MI' with MI.

23. (currently amended) The computer program recited in claim 19, wherein the gateway certificate generation code segment transmits a mobile subscriber identifier to the authentication ~~benter~~center, receives a random number, a signed response and an encryption key from the authentication center, computes a variable MI, M2', and M3 and verifies the validity of the mobile station by comparing variable M2 received from the mobile station with variable M2'.

24. (previously presented) A system for ordering, authorizing and delivering goods and services using a mobile station, comprising:

a mobile station;

a gateway, the mobile station accessing the gateway and transmitting an identification code for the mobile station to the gateway;

an authentication center, the authentication center being part of a cellular network, the gateway verifying the identity of the mobile station by accessing the authentication center and comparing mobile station generated variables computed by the mobile station with gateway generated variables computed by the gateway,

wherein the gateway delivers a digital certificate to the mobile station when the identity of the mobile station has been verified, the mobile station verifying the legitimacy of the gateway by comparing the variables computed by the gateway with

the variables computed by the mobile station and requesting a digital certificate from the gateway to be used to order and authorize a product or service from a service provider, the mobile station requesting a product or service from the service provider and transmitting a digital signature and the digital certificate for a signature verification key as authorization to the service provider.

25. (new) A mobile terminal, the mobile terminal capable of ordering goods and services from a service provider, comprising:

means for accessing a gateway and transmitting an identification code for the mobile terminal to the gateway;

means for generating variables and transmitting these variables to the gateway;

means for requesting a digital certificate from the gateway used to order and authorize a product or service from a service provider;

means for receiving a digital certificate from the gateway when the identity of the mobile terminal has been verified based on the generated variables;

means for requesting a product or service from the service provider; and

means for transmitting a digital signature accompanied by the digital certificate for a signature verification key as authorization to said service provider.